INFORMATION PROCESSOR AND METHOD THEREFOR

Patent number: JP2003224561

Publication date: 2003-08-08

Inventor: SLICK ROYCE E; ZHANG WILLIAM; PURPURA DON FRANCIS; IWAMOTO NEIL Y; MAZZAGATTE CRAIG

Applicant: CANON KK

Classification:

- international: H04L9/08; G06F3/12; G06F12/14

- european:

Application number: JP20020352937 20021204

Priority number(s): US20010010974 20011205

Also published as:

EP1320009 (A2)

US2003105963 (A1)

Abstract of **JP2003224561**

<P>PROBLEM TO BE SOLVED: To provide a constitution capable of securely holding a public key in a computing device which can easily verify the public key every time before use without the need of a certificate or an authentication authority. <P>SOLUTION: A secret key 54 intrinsic to a user is provided to a ciphering algorithm 65 together with a printer public key 25 to generate a ciphered printer public key 67 and it is stored in a registry 41 under the 'user 1' entry 42 of a sub entry 44. Then, before ciphering print data by using the printer public key 25, the already stored version of the printer public key 25 is authenticated. <P>COPYRIGHT: (C)2003,JPO

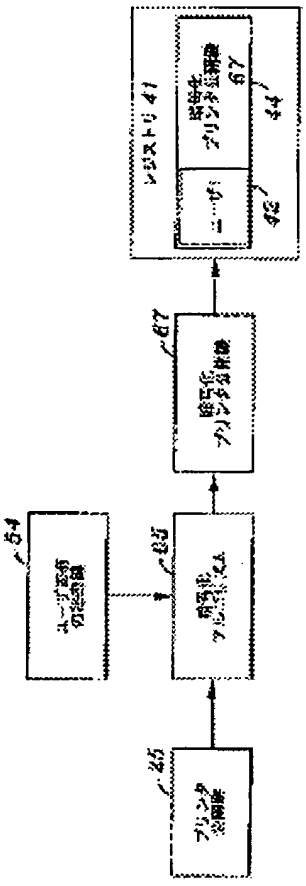

FIG.4A

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－224561
（P2003－224561A）
(43)公開日　平成15年８月８日(2003.8.8)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/08		G06F	3/12	K　5B017
G06F	3/12			12/14	320A　5B021
	12/14	320	H04L	9/00	601B　5J104
					601F

審査請求　有　　請求項の数32　ＯＬ　（全 22 頁）

(21)出願番号　特願2002－352937(P2002－352937)
(22)出願日　平成14年12月４日(2002.12.4)
(31)優先権主張番号　１０／０１０９７４
(32)優先日　平成13年12月５日(2001.12.5)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　ロイス　イー．スリック
アメリカ合衆国　カリフォルニア州　92612，アーバイン，イノベーション　ドライブ　110　キヤノン　デベロップメント　アメリカス，インコーポレイテッド内
(74)代理人　100076428
弁理士　大塚　康徳　（外３名）

最終頁に続く

(54)【発明の名称】　情報処理装置及びその方法

(57)【要約】
【課題】　証明書や認証局を必要とすることなく使用前に毎回、公開鍵を容易に検証できる計算装置において公開鍵を機密に保持できる構成が必要となる。
【解決手段】　ユーザ固有の秘密鍵５４をプリンタ公開鍵２５と共に暗号化アルゴリズム６５に提供して暗号化プリンタ公開鍵６７を生成し、これをサブエントリ４４の「ユーザ１」エントリ４２下にあるレジストリ４１に格納する。そして、プリンタ公開鍵２５を使用してプリントデータを暗号化する前に、プリンタ公開鍵２５の格納済みのバージョンを認証する。

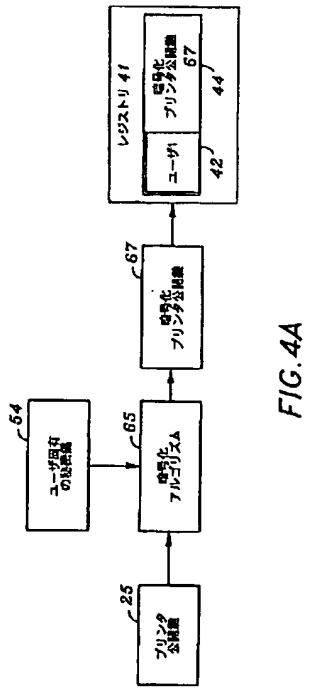

FIG. 4A

【特許請求の範囲】

【請求項１】　ユーザ固有の鍵対を使用し、且つ、データの暗号化のための公開鍵を用いてデータを暗号化する情報処理方法であって、
対象となる装置に対応する対象公開鍵を受信する受信工程と、
機密レジストリからユーザ固有の鍵対を取得する取得工程と、
前記ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して前記対象公開鍵に基づいて対象鍵を検証するためのデータ又はプログラムを作成する鍵暗号化工程と、
前記対象鍵を検証するためのデータ又はプログラムと前記対象公開鍵とを記憶領域に格納する格納工程と、
前記対象鍵を検証するためのデータ又はプログラムと前記対象公開鍵とを記憶領域から抽出する抽出工程と、
前記対象公開鍵の信頼性を検証するために、前記ユーザ固有の鍵対からのユーザ固有の公開鍵を前記対象鍵を検証するためのプログラム又はデータに適用する検証工程と、
前記対象公開鍵の信頼性が検証された場合、データを前記対象公開鍵で暗号化することによって前記対象となる装置に送信するための暗号化データを作成するデータ暗号化工程と、を有することを特徴とする情報処理方法。

【請求項２】　前記計算装置で実行するオペレーティングシステムがサポートする鍵を扱うためのアプリケーション・プログラミング・インタフェースを介して前記ユーザ固有の鍵対を取得することを特徴とする請求項１に記載の情報処理方法。

【請求項３】　前記オペレーティングシステムは、計算装置の複数のユーザのそれぞれに対してユーザ固有の鍵対を機密に保持することを特徴とする請求項２に記載の情報処理方法。

【請求項４】　各ユーザ固有の鍵対に対応するユーザ識別データをオペレーティングシステムに提供することによって前記ユーザ固有の鍵対にアクセスすることができることを特徴とする請求項２又は３に記載の情報処理方法。

【請求項５】　前記鍵暗号化工程で作成された前記対象鍵を検証するためのプログラム又はデータは、前記対象公開鍵の暗号化バージョンであることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理方法。

【請求項６】　前記検証工程は、復号化アルゴリズムを使用して前記ユーザ固有の公開鍵で前記対象鍵を検証するためのプログラム又はデータを復号化することを含むことを特徴とする請求項１乃至５のいずれか１項に記載の情報処理方法。

【請求項７】　前記検証工程は、前記対象公開鍵の信頼性を検証するために、鍵検証アルゴリズムを使用して前記復号化対象鍵を検証するためのプログラム又はデータと前記対象公開鍵とを比較することを更に含むことを特徴とする請求項６に記載の情報処理方法。

【請求項８】　前記計算装置で実行するオペレーティングシステムがサポートする検証用アプリケーション・プログラミング・インタフェースを介して前記検証工程を行うことを特徴とする請求項７に記載の情報処理方法。

【請求項９】　前記鍵暗号化工程で作成された前記対象鍵を検証するためのプログラム又はデータは、前記対象公開鍵のデジタル署名であることを特徴とする請求項１乃至８のいずれか１項に記載の情報処理方法。

【請求項１０】　ハッシングアルゴリズムを前記対象公開鍵に適用して対象鍵ハッシュを取得し、暗号化アルゴリズムを使用して前記対象鍵ハッシュを前記ユーザ固有の秘密鍵で暗号化することによって前記対象公開鍵のデジタル署名を作成することを特徴とする請求項９に記載の情報処理方法。

【請求項１１】　ハッシングアルゴリズムを前記対象公開鍵に適用して対象鍵ハッシュを取得し、前記対象鍵ハッシュに対して機密保護アルゴリズムを行うことによって前記対象公開鍵のデジタル署名を作成することを特徴とする請求項９に記載の情報処理方法。

【請求項１２】　前記検証工程は、復号化アルゴリズムを使用して前記対象鍵を検証するためのプログラム又はデータを前記ユーザ固有の公開鍵で復号化し、復号化対象鍵ハッシュを取得することを含むことを特徴とする請求項１１に記載の情報処理方法。

【請求項１３】　前記検証工程は、前記対象公開鍵の信頼性を検証するために、ハッシングアルゴリズムを前記対象公開鍵に再度適用して新たな対象鍵ハッシュを取得し、ハッシュ検証アルゴリズムを使用して前記復号化対象鍵ハッシュと前記新たな対象鍵ハッシュとを比較することを更に含むことを特徴とする請求項１２に記載の情報処理方法。

【請求項１４】　前記計算装置で実行するオペレーティングシステムがサポートする検証用アプリケーション・プログラミング・インタフェースによって前記検証工程を行うことを特徴とする請求項１３に記載の情報処理方法。

【請求項１５】　前記抽出工程は、前記受信した対象公開鍵の信頼性を検証するために、ハッシングアルゴリズムを前記受信した対象公開鍵に適用して受信した対象鍵ハッシュを取得し、ハッシュ検証アルゴリズムを使用して前記受信した対象鍵ハッシュとテスト用の対象鍵ハッシュとを比較することを含むことを特徴とする請求項１乃至１４のいずれか１項に記載の情報処理方法。

【請求項１６】　前記テスト用の対象鍵ハッシュはユーザによって入力されることを特徴とする請求項１５に記載の情報処理方法。

【請求項１７】　前記対象となる装置は画像形成装置であり、前記テスト用の対象鍵ハッシュを前記画像形成装置によって印刷されたテストページから取得することを

特徴とする請求項１６に記載の情報処理方法。
【請求項１８】　前記対象となる装置は画像形成装置であり、前記対象公開鍵は画像形成装置公開鍵であることを特徴とする請求項１乃至１７のいずれか１項に記載の情報処理方法。
【請求項１９】　前記受信工程において、前記画像形成装置に送られた鍵要求に応じて前記画像形成装置公開鍵を受信することを特徴とする請求項１８に記載の情報処理方法。
【請求項２０】　前記情報処理方法は、前記計算装置で実行するプリンタドライバによって行われることを特徴とする請求項１８に記載の情報処理方法。
【請求項２１】　ユーザ固有の鍵対を使用し且つ、プリントデータの暗号化のためのプリンタ公開鍵を前記計算装置に機密に格納する情報処理方法において、
プリンタに対応するプリンタ公開鍵を受信する受信工程と、
対応するユーザ識別に応じて機密レジストリからユーザ固有の鍵対を取得する取得工程と、
ハッシングアルゴリズムを前記プリンタ公開鍵に適用して第１のプリンタ鍵ハッシュを作成する第１のハッシング工程と、
暗号化アルゴリズムを適用して前記ユーザ固有の鍵対からのユーザ固有の秘密鍵で前記第１のプリンタ鍵ハッシュを暗号化することよってプリンタ鍵署名を作成する暗号化工程と、
前記プリンタ鍵署名と前記プリンタ公開鍵とを記憶領域に格納する格納工程と、
前記プリンタ鍵署名と前記プリンタ公開鍵とを記憶領域から抽出する抽出工程と、
前記ハッシングアルゴリズムを前記抽出したプリンタ公開鍵に適用して第２のプリンタ鍵ハッシュを作成する第２のハッシング工程と、
復号化アルゴリズムを適用して前記ユーザ固有の鍵対からのユーザ固有の公開鍵で前記プリンタ鍵署名を復号化することによって前記第１のプリンタ鍵ハッシュを抽出する復号化工程と、
前記抽出したプリンタ公開鍵の信頼性を検証するために、検証アルゴリズムを適用して前記第１のプリンタ鍵ハッシュと前記第２のプリンタ鍵ハッシュとを比較する検証工程と、
前記抽出したプリンタ公開鍵の信頼性が検証された場合、前記抽出したプリンタ公開鍵を使用して暗号化アルゴリズムをプリントデータに適用することによって前記プリンタに送信するための暗号化プリントデータを作成するプリントデータ暗号化工程と、を有することを特徴とする情報処理方法。
【請求項２２】　計算装置で受信した画像形成装置の公開鍵の信頼性を検証する情報処理方法において、
画像形成装置に対応する画像形成装置の公開鍵を前記計算装置で受信する第１の受信工程と、
ハッシングアルゴリズムを前記画像形成装置の公開鍵に適用して第１の画像形成装置の鍵ハッシュを作成するハッシング工程と、
前記画像形成装置で印刷されたテストページから取得し、前記計算装置に接続したユーザ入力手段で前記計算装置に入力する所定の第２の画像形成装置の鍵ハッシュを前記計算装置で受信する第２の受信工程と、
前記受信した画像形成装置の公開鍵の信頼性を検証するために、検証アルゴリズムを適用して前記第１の画像形成装置の鍵ハッシュと前記第２の画像形成装置の鍵ハッシュとを比較する検証工程と、
前記受信した画像形成装置の公開鍵の信頼性が前記検証工程で検証された場合、前記受信した画像形成装置の公開鍵を前記計算装置の記憶領域に格納する格納工程と、を有することを特徴とする情報処理方法。
【請求項２３】　データの暗号化のための公開鍵を認証する装置において、
請求項１から２２のいずれか１項に記載の情報処理方法を行うために実行可能な処理工程を格納するプログラムメモリと、
前記プログラムメモリに格納された処理工程を実行するプロセッサと、を有することを特徴とする装置。
【請求項２４】　データの暗号化のための公開鍵を認証するためのコンピュータ可読媒体に格納されたコンピュータにより実行可能な情報処理方法であって、
請求項１から２２のいずれか１項に記載の情報処理方法を行うために実行可能である処理工程を含むことを特徴とする情報処理方法。
【請求項２５】　データの暗号化のための公開鍵を認証するためのコンピュータ実行可能な処理工程を格納するコンピュータ可読媒体において、
前記コンピュータ実行可能な処理工程は請求項１から２２のいずれか１項に記載の情報処理方法を実施可能である処理工程を有することを特徴とする可読媒体。
【請求項２６】　データの暗号化のための公開鍵を機密に格納し、情報装置に機密に格納されたユーザ固有の鍵対を利用し且つ、暗号化データを対象となる装置に送信する情報処理装置であって、
対象となる装置に対応する対象公開鍵を受信する受信手段と、
機密レジストリからユーザ固有の鍵対を取得する取得手段と、
前記ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して前記対象公開鍵に基づいて対象鍵を検証するためのプログラム又はデータを作成する鍵暗号化手段と、
前記対象鍵を検証するためのプログラム又はデータと前記対象公開鍵とを格納する格納手段と、
前記対象鍵を検証するためのプログラム又はデータと前記対象公開鍵とを前記格納手段から抽出する抽出手段

と、
前記対象公開鍵の信頼性を検証するために、前記ユーザ固有の鍵対からのユーザ固有の公開鍵を前記対象鍵を検証するためのプログラム又はデータに適用する検証手段と、
前記対象公開鍵の信頼性が検証された場合、データを前記対象公開鍵で暗号化することによって前記対象となる装置に送信するための暗号化データを作成するデータ暗号化手段と、を有することを特徴とする情報処理装置。
【請求項２７】　暗号化プリントデータを画像形成装置に転送する情報処理装置であって、
前記画像形成装置から公開鍵を抽出する抽出手段と、
前記公開鍵から検証情報を生成する生成手段と、
印刷命令を認識する認識手段と、
前記印刷命令の認識に応答して、前記公開鍵が前記抽出した公開鍵から変更していないことを検証する検証手段と、
前記抽出した公開鍵が変更していないと検証された場合に、前記公開鍵を使用して暗号化処理を行い、前記抽出した公開鍵が変更したと検証された場合に暗号化処理を行わないように暗号化処理を制御する制御手段と、を有することを特徴とする情報処理装置。
【請求項２８】　コンピュータに格納したユーザ固有の鍵を取得する取得手段と、
認証情報を入力する入力手段と、
前記取得手段が前記ユーザ固有の鍵を取得可能かどうかを判定する判定手段とを更に具備することを特徴とする請求項２７に記載の情報処理装置。
【請求項２９】　前記制御手段は暗号化処理を制御し、取得手段で取得したユーザ固有の鍵を使用してプリントデータを暗号化し、前記公開鍵を使用して前記ユーザ固有の鍵を暗号化することを特徴とする請求項２７に記載の情報処理装置。
【請求項３０】　暗号化プリントデータを画像形成装置に転送する情報処理方法であって、
前記画像形成装置から公開鍵を抽出する抽出工程と、
前記公開鍵から検証情報を生成する生成工程と、
印刷命令を認識する認識工程と、
前記印刷命令の認識に応じて、前記公開鍵が前記抽出した公開鍵から変更していないことを検証する検証工程と、
前記抽出した公開鍵が変更していないと検証された場合に前記公開鍵を使用して暗号化処理を行い、前記抽出した公開鍵が変更したと検証された場合に暗号化処理を行わないように暗号化処理を制御する制御工程と、を有することを特徴とする情報処理方法。
【請求項３１】　コンピュータに格納したユーザ固有の鍵を取得する取得工程と、
認証情報を入力する入力工程と、
前記取得工程で前記ユーザ固有の鍵を取得可能かどうかを判定する判定工程とを更に含むことを特徴とする請求項３０に記載の情報処理方法。
【請求項３２】　前記制御工程は暗号化処理を制御し、取得工程で取得したユーザ固有の鍵を使用してプリントデータを暗号化し、前記公開鍵を使用して前記ユーザ固有の鍵を暗号化することを特徴とする請求項３０又は３１に記載の情報処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理装置、方法、制御プログラムにおける暗号化処理に関するものである。
【０００２】［文献の援用］１９９９年１０月４日出願の米国特許出願第０９／４１１，０７０号、名称「Targeted Secure Printing」を文献として援用する。
【０００３】
【従来の技術】計算環境では、ネットワーク上の１箇所にあるコンピュータで生成された印刷ジョブを、他の場所にある画像出力装置で印刷することができる。例えば、パーソナルコンピュータ（ＰＣ）を離れた場所にあるプリンタに接続しても良いし、ワークステーションを多数の装置やワークステーションが存在するネットワークに接続しても良い。印刷ジョブが機密情報や他の取り扱いに注意を要する情報を含んでいる場合、印刷ジョブの発信元と送信先のプリンタとの間で印刷ジョブが無許可で傍受されてしまう可能性がある。特に、発信元のＰＣと送信先のプリンタとの間のローカル接続に接続されている無許可の装置や、発信元のワークステーションと送信先のプリンタとが存在するネットワークに接続されている装置によって印刷ジョブが傍受されてしまう可能性がある。このような無許可の装置は、ネットワーク盗聴ツール、ネットワークトラッピングツール、及びネットワーク傍受ツールを利用可能なＰＣやワークステーションであるかもしれない。
【０００４】印刷ジョブの望ましくない傍受や抽出を回避するために、プリンタ公開鍵を利用して発信元のコンピュータでプリントデータを暗号化する機密印刷を使用することが知られている。プリンタ公開鍵を対称鍵と共に使用してプリントデータを暗号化するアプリケーションもある。暗号化プリントデータは送信先のプリンタに送られて、そこでプリンタ公開鍵を使用してプリントデータを復号化し格納する。プリンタ公開鍵はプリンタで機密に保持されて、暗号化プリントデータの機密保護を確実なものにする。コンピュータが画像形成装置の好適な一例であるプリンタ公開鍵を取得して格納することが好ましいが、プリンタ公開鍵が改変又は改竄されていないことを確認するために、プリンタ公開鍵を使用してプリントデータを暗号化する度にプリンタ公開鍵を検証するべきである。
【０００５】暗号化処理用の公開鍵の機密配布及び検証

を容易にするために認証局を使用することが多い。認証局とは、ユーザへの機密配信のためにプリンタ製造業者などの開発者や製造業者に対して固有の公開鍵を署名できる第三者機関である。例えば、認証局は、プリンタ公開鍵の配信元と認証局とに関する情報と共に配信用の証明書にプリンタ公開鍵を添付して、証明書全体に署名することによって、認証局自身の秘密鍵を使用してプリンタ製造業者からのプリンタ公開鍵に署名できる。その後、ユーザは、使用する署名後のプリンタ公開鍵を含む証明書にアクセスできる。このような場合、ユーザは認証局自身の信用公開鍵（検証鍵）を取得して、この公開鍵を使用して署名されたプリンタ公開鍵が正規のものであることを検証する。それによって、対応するプリンタ秘密鍵を含む送信先のプリンタで印刷するユーザのプリントデータの暗号化に対して、ユーザがプリンタ公開鍵を信用することが可能となる。

【０００６】プリンタ公開鍵などの装置の公開鍵の使用を望むユーザが認証局からの証明書を利用して公開鍵の信頼性を検証することは実用的でないことが多い。例えば、認証局は、証明書の保全性を維持するために時々その検証鍵を変更することが知られている。更に、証明書が期限切れになるか、又は認証局によって無効になる可能性もある。証明書の保全性を確実なものにするには、証明書の保全性を信頼する前に認証廃棄リスト（ＣＲＬ）をチェックしなければならない。残念ながら、暗号化処理に対して特定の公開鍵を使おうとしている際に、毎回、ユーザが認証局の検証鍵を取得することは時間がかかってしまう。

【０００７】加えて、全ての装置がその公開鍵の配信に認証局を使用するとは限らない。また、ユーザは、ユーザのアプリケーション毎に必要となる異なる公開鍵をサポートするための対応する認証局からの多数の検証鍵を格納して保持しなければならない可能性もある。最後に、認証局からの証明書は署名された公開鍵に加えて付加情報を含んでいることが多く、この付加情報を処理することで、署名された公開鍵の検証時の処理のオーバーヘッドが増加してしまう。

【０００８】

【発明が解決しようとする課題】そのため、証明書や認証局を必要とすることなく使用前に毎回、公開鍵を容易に検証できる計算装置において公開鍵を機密に保持できる構成が必要となる。

【０００９】本発明は、プリンタなどの対象となる装置から公開鍵を取得して格納することによって、上記の問題を解決する。ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して、公開鍵に対応する対象鍵を検証するためのデータ又はプログラムを作成する。これに関して、対象鍵を検証するためのデータ又はプログラムとしては、本発明の目的に応じた複数の種類のデータオブジェクトのいずれか１つが可能である。例えば、対象鍵を検証するためのデータ又はプログラムは、暗号化公開鍵、公開鍵のデジタル署名、又はＤＳＳなどの機密保護アルゴリズムを公開鍵に適用して得られる他のデータオブジェクトから構成することが可能である。公開鍵が暗号化のために引き続き必要となる場合は、ユーザ固有の鍵対からのユーザ固有の公開鍵を使用して対象鍵を検証するためのデータ又はプログラムを復号化し、格納済みの公開鍵と比較することで、格納済みの公開鍵が変更又は改変されていないことを検証する。

【００１０】

【課題を解決するための手段】そのため、本発明の一態様は、計算装置に機密に格納したユーザ固有の鍵対を使用して、計算装置のデータの暗号化のための公開鍵を機密に格納することに関する。特に、対象となる装置に対応する対象公開鍵を受信し、機密レジストリからユーザ固有の鍵対を取得し、ユーザ固有の鍵対からのユーザ固有の秘密鍵を使用して前記対象公開鍵に基づいて対象鍵を検証するためのデータ又はプログラムを作成する。対象鍵を検証するためのデータ又はプログラムと対象公開鍵とを記憶領域に格納する。続いて、対象鍵を検証するためのデータ又はプログラムと対象公開鍵とを記憶領域から抽出する。対象公開鍵の信頼性を検証するために、ユーザ固有の鍵対からのユーザ固有の公開鍵を対象鍵を検証するためのデータ又はプログラムに適用し、対象公開鍵の信頼性が検証された場合、データを対象公開鍵で暗号化することによって対象となる装置に送信するための暗号化データを作成する。

【００１１】計算装置で実行するオペレーティングシステムが、ユーザ固有の鍵対を生成し機密に保持するのが好ましい。例えば、オペレーティングシステムは、各ユーザのユーザ固有の鍵対を格納し、ユーザ固有の鍵対に対応するユーザの適切なログイン識別が提供された時のみユーザ固有の鍵対へのアクセスを許可する機密レジストリを保持するのが好ましい。また、対象鍵を検証するためのデータ又はプログラムは、対象公開鍵をハッシングし、ユーザ固有の鍵対からのユーザ固有の秘密鍵で第１の鍵ハッシュを暗号化することによって作成された公開鍵署名であるのが好ましい。検証工程は、ユーザ固有の鍵対からのユーザ固有の公開鍵で対象鍵を検証するためのデータ又はプログラムを復号化して第１の鍵ハッシュを抽出することを含むのが好ましい。格納済みの対象公開鍵をハッシングして第２の鍵ハッシュを取得し、第１及び第２の鍵ハッシュを比較して、格納済みの対象公開鍵の信頼性を検証する。また、受信工程において、計算装置から対象となる装置への要求に応じて対象公開鍵を受信するのが好ましい。

【００１２】上述の構成によって、データの暗号化で引き続き使用するために計算装置で対象公開鍵を機密に保持することができる。特に、対象公開鍵の暗号化（署名）とそれ以降の検証を局所的に保持されたユーザ固有

の鍵対で行うことによって、外部のデジタル証明書や認証局を必要とすることなく、使用する前に毎回、対象公開鍵を検証することが容易になる。

【００１３】他の態様では、本発明は、計算装置に機密に格納したユーザ固有の鍵対を使用して、画像形成データの暗号化のための画像形成装置の公開鍵を計算装置に機密に格納することに関する。特に、画像形成装置に対応する画像形成装置の公開鍵を受信し、対応するユーザ識別に応じて機密レジストリからユーザ固有の鍵対を取得する。ハッシングアルゴリズムを画像形成装置の公開鍵に適用して第１の画像形成装置鍵ハッシュを作成し、暗号化アルゴリズムを適用してユーザ固有の鍵対からのユーザ固有の秘密鍵で第１の画像形成装置鍵ハッシュを暗号化することよって画像形成装置の鍵署名を作成する。この画像形成装置の鍵署名と画像形成装置の公開鍵とを記憶領域に格納する。続いて、画像形成装置の鍵署名と画像形成装置の公開鍵とを記憶領域から抽出する。ハッシングアルゴリズムを抽出した画像形成装置の公開鍵に適用して第２の画像形成装置の鍵ハッシュを作成し、復号化アルゴリズムを適用してユーザ固有の鍵対からのユーザ固有の公開鍵で画像形成装置の鍵署名を復号化することによって第１の画像形成装置の鍵ハッシュを抽出する。抽出した画像形成装置の公開鍵の信頼性を検証するために、検証アルゴリズムを適用して前記第１の画像形成装置の鍵ハッシュと第２の画像形成装置の鍵ハッシュとを比較し、抽出した画像形成装置の公開鍵の信頼性が検証された場合、抽出した画像形成装置の公開鍵を使用して暗号化アルゴリズムを画像形成データに適用することによって画像形成装置に送信するための暗号化プリントデータを作成する。

【００１４】計算装置で実行するオペレーティングシステムが、取得工程で取得したユーザ固有の鍵対を生成し機密に保持するのが好ましい。例えば、オペレーティングシステムは、各ユーザのユーザ固有の鍵対を格納し、ユーザ固有の鍵対に対応するユーザの適切なログイン識別が提供された時のみユーザ固有の鍵対へのアクセスを許可する機密レジストリを保持するのが好ましい。また、受信工程において、計算装置から画像形成装置へ送られる鍵要求に応じて画像形成装置の公開鍵を受信するのが好ましい。

【００１５】上述の構成によって、データの暗号化で引き続き使用するために計算装置で画像形成装置の公開鍵を機密に保持することができる。特に、画像形成装置の公開鍵の署名とそれ以降の検証を局所的に保持されたユーザ固有の鍵対で行うことによって、外部のデジタル証明書や認証局を必要とすることなく、使用する前に毎回、画像形成装置の公開鍵を検証することが容易になる。

【００１６】本発明の更に他の態様によると、計算装置が受信した画像形成装置の公開鍵を認証する。特に、計算装置は画像形成装置に対応する画像形成装置の公開鍵を受信し、ハッシングアルゴリズムを画像形成装置の公開鍵に適用して第１の画像形成装置の鍵ハッシュを作成する。計算装置は、画像形成装置で印刷されたテストページから取得した所定の第２の画像形成装置の鍵ハッシュを受信する。この第２の画像形成装置の鍵ハッシュは、計算装置に接続したユーザ入力手段で計算装置に入力される。受信した画像形成装置の公開鍵の信頼性を検証するために、検証アルゴリズムを適用して第１の画像形成装置の鍵ハッシュと第２の画像形成装置の鍵ハッシュとを比較し、受信した画像形成装置の公開鍵の信頼性が検証された場合、受信した画像形成装置の公開鍵を計算装置の記憶領域に格納する。

【００１７】受信した画像形成装置の公開鍵は、計算装置から画像形成装置に送られた鍵要求メッセージに応じて受信するのが好ましい。加えて、テストページは計算装置のユーザからのコマンドに応じて印刷するのが好ましく、このコマンドは画像形成装置の前面パネルを介してユーザによって直接入力される。ユーザ入力手段はキーボードかマウスであるのが好ましく、これによってユーザはテストページから所定の第２のプリンタ鍵ハッシュを見ることができ、所定の第２の画像形成装置の鍵ハッシュを計算装置に入力することができる。

【００１８】上述の構成によって、画像形成装置の公開鍵を画像形成装置から画像形成装置のユーザで最初に受信された後に認証することができる。特に、ユーザが存在する場合、受信した画像形成装置の公開鍵の認証を、画像形成装置で印刷された所定のハッシュ値を使用して行う。このように、外部のデジタル証明書や認証局を必要とすることなく、画像形成装置の公開鍵の信頼性を受信後に容易に検証する。

【００１９】本発明の性質を即座に理解できるように、本発明の簡単な概要を提示した。添付の図面と関連させて以下の好ましい実施例の詳細な説明を参照することにより、本発明をより完全に理解することができるであろう。

【００２０】

【発明の実施の形態】本実施形態は、他のデータ処理装置にも適用可能であるが、外部の認証局を必要とすることなく、検証済みのプリンタ鍵を使用してプリントデータを暗号化する機密印刷を行う環境を提供する。特に、本実施形態は、ユーザ固有の秘密鍵を使用して格納済みのプリンタ公開鍵の暗号化鍵バージョンを作成する。プリンタ公開鍵がプリントデータの暗号化のために引き続き必要となる場合は、暗号化鍵バージョンをユーザ固有の公開鍵を使用して復号化した後、格納済みのプリンタ公開鍵と比較して、格納済みのプリンタ公開鍵が変更又は改変されていないことを検証することになる。図１は、本発明の実施の形態を実現する計算環境のシステム図である。図１に示すように、計算環境は、コンピュー

タ１０と、プリンタ２０と、接続１とを備える。接続１としては、シリアル接続、ＵＳＢ接続、ファイアワイヤ接続又は他の接続などのコンピュータ１０とプリンタ２０との間の単純なローカル接続が可能である。代わりに、接続１は、バス型物理構造から成るイーサネットネットワーク媒体などのネットワークでも良い。接続１をインターネットを含む他の種類のネットワークで構成しても良いことは理解されるであろう。

【００２１】デスクトップコンピュータ１０は、MicrosoftＷｉｎｄｏｗｓ（登録商標）2000, MicrosoftWindows ME又はMicrosoftWindows XPなどのウィンドウイングオペレーティングシステム環境を有するパーソナルコンピュータやワークステーションであるのが好ましい。ＰＣコンピュータの典型的として、デスクトップコンピュータ１０は、ディスプレイ１１と、キーボード１５と、マウス１４と、ホストプロセッサ１２と、固定ディスク１３と、フロッピー（登録商標）ドライブ及び／又は他の種類の記憶媒体（不図示）を有することが好ましい。本実施の形態に係る固定ディスク１３の内容とコンピュータ１０の動作は以下に更に詳述する。

【００２２】プリンタ２０も接続１によってコンピュータ１０に接続されており、受信したプリントデータに基づいて記録媒体に画像を印刷できるレーザプリンタ又はインクジェットプリンタが好ましい。プリンタ２０は、好ましくは固定ディスクである固定記憶装置２１を有するが、ＲＯＭやＥＥＰＲＯＭなどの他の形式のコンピュータメモリでも良い。本実施の形態に係る固定記憶装置２１の内容とプリンタ２０の動作は以下に更に詳述する。

【００２３】図２は、本実施の形態に係るネットワーク化計算環境のシステム図である。図２に示すように、計算環境は、コンピュータ１０と、プリンタ２０と、サーバ３０と、接続１とを備える。図２のコンピュータ１０とプリンタ２０は、図１を参照して説明したものと同じである。しかし、図２の接続１は、バス型物理構造から成るイーサネット（登録商標）ネットワーク媒体などのネットワーク接続であるのが好ましい。

【００２４】図２に示すように、サーバ３０も接続１に接続されている。サーバ３０は、Microsoft Windows（登録商標）2000, Microsoft Windows（登録商標） ME又はMicrosoft（登録商標）Windows XPなどのウィンドウイングオペレーティングシステム環境を有するＰＣ互換型コンピュータを備えることが好ましい。サーバ３０は、多数のファイル、アプリケーション、及びデータを格納する大型固定ディスクであるのが好ましい固定ディスク３１を有する。従って、サーバ３０をファイルサーバ、又はプリントサーバなどの他の種類のサーバとして、コンピュータ１０などの接続１上の他の装置で利用することができる。また、サーバ３０は、接続１上の他の装置がインターネットなどの他のネットワークにアクセスするためのゲートウェイとして機能しても良い。本発明の一実施の形態では、以下に更に詳述するように、サーバ３０を使用してコンピュータ１０が使用する公開鍵を格納する。

【００２５】図３は、コンピュータ１０の固定ディスク１３の内容及びプリンタ２０の固定記憶装置２１の内容を説明する図である。本発明はプリンタ以外の装置で実施することもできるが、ここではプリンタと共に使用する場合の本実施の形態を述べる。図３に示すように、プリンタ２０の固定記憶装置２１は、プリンタ公開鍵２５とプリンタ秘密鍵２３とを含むプリンタ鍵対２２を含む。鍵２５と２３は、プリントデータの暗号化及び復号化にそれぞれ使用する暗号化鍵である。特に、プリンタ公開鍵２５は、プリンタ２０の製造業者が作成して保持するのが好ましいが、プリンタ２０のシステム管理者や他のシステムユーザがプリンタ２０にインストールすることもできる。代わりに、プリンタ２０自身がプリンタ公開鍵２５を生成することもできる。

【００２６】プリンタ公開鍵２５は、機密暗号化方式でプリンタ２０に送るプリントデータの暗号化で使用するために一般の人々がアクセスできるようになっている。プリンタ秘密鍵２３もプリンタ公開鍵２５に対応する暗号化鍵であり、プリンタ公開鍵２５の作成者によって作成される。しかし、プリンタ秘密鍵２３はプリンタ２０内で厳密な機密保護の下に保持されており、プリンタ公開鍵２５のようにアクセスすること及び／又はプリンタ２０から削除することはできない。このように、プリンタ鍵対２２の鍵２３と２５の両方にプリンタ２０のみがアクセスすることができるので、暗号化プリントデータがプリンタ２０に向かう途中で傍受されても、プリンタ２０に送られた暗号化プリントデータを無許可の第三者が復号化することはできないことをプリンタ２０のユーザに信用させることができる。

【００２７】図３に戻ると、コンピュータ１０の固定ディスク１３が、オペレーティングシステム４０と、レジストリ４１と、鍵データベース５０と、プリンタドライバ６０と、記憶領域６２とを含んでいることが判る。前述のように、オペレーティングシステム４０はウィンドウイングオペレーティングシステムであるのが好ましく、特に暗号化アプリケーションプログラミングインタフェース（ＣＡＰＩ）を含むMicrosoftWindows（登録商標）オペレーティングシステムであるのが好ましい。例えば、Microsoft CAPIは、効率的なトランスペアレント方式でユーザ固有の暗号化鍵対を生成し、保持し、アクセスするトランスペアレント方式を提供する。特に、ＣＡＰＩはコンピュータ１０のユーザ毎にユーザ固有の鍵対を生成し、特定の対応するユーザに対して各ユーザ固有の鍵対をレジストリエントリに格納する。ＣＡＰＩ（Crypto API）では、対応するユーザがユーザ固有のパスワードなどの適切なユーザログイン識別を提供するこ

とでコンピュータ１０にログインしたのでない限り、ユーザ固有の鍵対へのアクセスを許可しない。許可されたユーザに対してユーザ固有の鍵対を検索するために、ＣＡＰＩは関数呼出しをサポートしている。また、ＣＡＰＩは、ユーザ固有の公開鍵で暗号化又は署名された公開鍵などのデータの信頼性を検証するための関数呼出しなど、他の暗号化関数呼出しもサポートする。

【００２８】データの暗号化署名やそれ以降の暗号化署名の検証をサポートするＰＧＰなどのアプリケーションも存在するが、このようなアプリケーションはMicrosoftWindows CAPIの機能性に対して著しい欠点を有しているように見える。特に、ＰＧＰなどの他の暗号化アプリケーションでは、暗号化署名の作成に使用する鍵対の記憶をアプリケーションのユーザが保持しなければならない。そのため、このようなアプリケーションでは厳密な機密保護の下で鍵対を保持するわけではないので、コンピュータの無許可のユーザが鍵対にアクセスして使用することで、許可されたユーザの暗号化データにアクセスできてしまう機密保護侵害を起こす可能性が高くなる。

【００２９】ＣＡＰＩをサポートするMicrosoftWindowsオペレーティングシステムを使用するのが好ましいが、他の種類のオペレーティングシステムを使用して本発明を実施できることは理解されるであろう。このような場合、ＣＡＰＩで説明したように、ユーザにトランスペアレントな機密方式でユーザ固有の鍵対を生成し、保持し、アクセスする限り、上述のユーザ固有の鍵対の生成、保持、及びアクセスを他の種類のオペレーティングシステムの機能によって行うことができるし、アプリケーションによって行うこともできる。

【００３０】図３に戻ると、鍵データベース５０はオペレーティングシステム４０の構成要素であり、コンピュータ１０のユーザに対してユーザ固有の鍵対を機密に生成して保持するのに使用する。特に、鍵データベース５０はコンピュータ１０の各ユーザに対するユーザエントリを含んでおり、各ユーザエントリは「ユーザ１」５１に対応するエントリ中のユーザ固有の鍵対５１などの対応するユーザ固有の鍵対を含む。各ユーザ固有の鍵対は、データオブジェクトの暗号化／署名と暗号化／署名されたデータオブジェクトの信頼性の検証に対する秘密鍵と公開鍵とを含む。例えば、ユーザ固有の鍵対５１はユーザ固有の公開鍵５３とユーザ固有の秘密鍵５４とを含んでおり、これらは共に「ユーザ１」５１に固有のものであり、且つこれに対応している。

【００３１】レジストリ４１は、コンピュータ１０の各ユーザに対応するデータを保持するためにオペレーティングシステム４０が使用する記憶領域である。特に、レジストリ４１は各ユーザに対するエントリを含んでおり、このエントリにはログイン識別データが格納されており、他のユーザ固有のデータも格納されている。例えば、レジストリ４１のユーザ１（４２）に対するエントリはログインＩＤ４５とデジタル署名４４とを含む。ログインＩＤ４５は、コンピュータ１０にログインするためにユーザ１が使用し、機密保護のためにユーザ１だけが知っているパスワードであるのが好ましい。デジタル署名４４はプリンタ公開鍵２５などの対象となる鍵の信頼性を検証するためのプログラム及びデータを含む対象鍵ベリファイアである。デジタル署名４４は、ユーザ１に対応するユーザ固有の鍵対５１によって作成されてレジストリ４１に保持されるデジタル署名であるのが好ましい。代わりに、デジタル署名４４を対象鍵の暗号化バージョンで構成することもできるし、ＤＳＳなどの機密保護アルゴリズムを対象鍵に適用して得られたコードで構成することもできる。デジタル署名４４は以下に更に詳述する。

【００３２】同じく図３に示されるように、プリンタドライバ６０を使用して、テキスト文書、映像、図形、又は他の種類の画像であるような画像の印刷を行うためにプリンタ２０に送られるプリントデータを生成する。プリンタドライバ６０は、最適な印刷品質を確保してプリンタ２０の特徴と特性をサポートするためにプリンタ２０に対応するのが好ましい。本発明の好適な実施の形態では、以下に更に詳述するように、プリンタドライバ６０は本実施の形態の機能性を実現するためのソフトウェアコードを含む。

【００３３】図３の記憶領域６２は、プリンタドライバ６０がアクセスするための固定ディスク１３の通常の記憶領域であるが、必ずしも機密でなくても良い。記憶領域６２は、プリンタ公開鍵２５と、暗号化（署名）アルゴリズム６５と、ハッシングアルゴリズム６８と、復号化（検証）アルゴリズム７６と、鍵検証アルゴリズム７７と、ハッシュ検証アルゴリズム８４と、その他のアプリケーション５８と、その他のファイル５９とを含む。以下に更に説明するように、プリンタ公開鍵２５はプリントデータを暗号化する際に使用するためにプリンタ２０から取得した。

【００３４】暗号化（署名）アルゴリズム６５は、プリントデータやプリンタ公開鍵２５などのデータオブジェクトを暗号化又はデジタル署名するためにプリンタドライバ６０が使用する。加えて、本実施の形態に係る暗号化（署名）アルゴリズム６５は、他の種類の機密保護アルゴリズムで構成することができる。ハッシングアルゴリズム６８は、以下に更に説明するように、プリンタ公開鍵２５などのデータオブジェクトのデジタルハッシュを行うために使用する。復号化（検証）アルゴリズム７６は、以下に更に説明するように、プリンタ公開鍵２５などの暗号化データオブジェクトを復号化したり、署名されたデータオブジェクトのデジタル署名を検証するために使用する。加えて、本実施の形態に係る復号化（検証）アルゴリズム７６は、他の種類の機密保護アルゴリズムで構成することができる。鍵検証アルゴリズム７７

は、以下に更に十分に説明するように、復号化公開鍵と格納済みの公開鍵とを比較して、格納済みの公開鍵の信頼性を確認するために使用する。ハッシュ検証アルゴリズム８４は、以下に更に十分に説明するように、復号化公開鍵のハッシュ値と格納済みの公開鍵に対して新たに生成されたハッシュ値とを比較して、格納済みの公開鍵の信頼性を確認するために使用する。最後に、その他のアプリケーション５８とその他のファイル５９は、その他のアプリケーションと機能をサポートするためにプリンタドライバ６０及び／又はコンピュータ１０が使用する。

【００３５】図４Ａは、本発明の一実施の形態に係るプリンタ公開鍵２５を機密に格納する方法を示すブロック図である。まず、プリンタ公開鍵２５は、コンピュータ１０からの鍵要求に応じてプリンタ２０から取得するのが好ましい。図２に示す代替環境では、プリンタ公開鍵２５は、コンピュータ１０からの鍵要求に応じてサーバ３０から取得することができる。サーバ３０は、プリンタ公開鍵２５をプリンタ２０から事前に取得している。図４Ａに示すように、ユーザ固有の秘密鍵５４をプリンタ公開鍵２５と共に暗号化アルゴリズム６５に提供して暗号化プリンタ公開鍵６７を生成し、これをサブエントリ４４中の「ユーザ１」エントリ４２下にあるレジストリ４１に格納する。前述のように、ユーザ固有の秘密鍵５４には、ユーザ１のログインＩＤ４５に基づいてオペレーティングシステム４０を介してアクセスするのが好ましい。このように、今後も使用するためにプリンタ公開鍵２５を暗号化された方式でレジストリ４１に機密に格納し、プリンタ公開鍵２５を使用してプリントデータを暗号化する前にプリンタ公開鍵２５の格納済みのバージョンを認証する。

【００３６】図４Ｂは、プリンタ公開鍵２５を完全に暗号化する代わりにデジタル署名する本発明の他の実施の形態を示す。署名は完全な暗号化よりも処理のオーバーヘッドが少ないので、署名方法は完全暗号化方法より好ましい。図４Ｂに示すように、まず、コンピュータ１０の計算環境に応じてプリンタ公開鍵２５をプリンタ２０から直接取得するか又はサーバ３０から取得する。その後、プリンタ公開鍵２５に固有のプリンタ公開鍵ハッシュ値６９を生成するデジタルハッシングアルゴリズム６８を、プリンタ公開鍵２５に対して行う。ハッシングアルゴリズム６８は、ハッシングアルゴリズムを適用するデータオブジェクトに対応するハッシュ値を作成する既存の種類のハッシングアルゴリズムであるのが好ましい。

【００３７】ユーザ固有の秘密鍵５４をプリンタ公開鍵ハッシュ値６９と共に暗号化アルゴリズム６５に提供し、基本的にプリンタ公開鍵ハッシュ値６９の暗号化形式であるデジタル署名７０を作成する。その後、デジタル署名７０は、サブエントリ４４中の「ユーザ１」エントリ４２下にあるレジストリ４１に格納される。前述のように、ユーザ固有の秘密鍵５４には、ユーザ１のログインＩＤ４５に基づいてオペレーティングシステム４０を介してアクセスするのが好ましい。このように、デジタル署名７０を今後も使用するためにレジストリ４１に機密に格納し、プリンタドライバ６０がプリンタ公開鍵２５を使用してプリントデータを暗号化する前にプリンタ公開鍵２５の格納済みのバージョンを認証する。

【００３８】図５Ａは、プリンタ公開鍵２５の使用に先立ってプリンタ公開鍵２５の信頼性を検証するために図４Ａに示すように作成して格納した暗号化プリンタ公開鍵６７の使用を示すブロック図である。図５Ａにおいて、印刷コマンド７２はコンピュータ１０のユーザから受信するが、所望のプリントデータを機密にプリンタ２０に送るという指示を含んでいるのが好ましい。図５Ａに示すように、ユーザ固有の公開鍵５３には、前述のようにオペレーティングシステム４０を介してアクセスするのが好ましい。ユーザ固有の公開鍵５３を暗号化プリンタ公開鍵６７と共に復号化アルゴリズム７６に提供して復号化プリンタ公開鍵７５を取得する。プリンタ公開鍵２５は記憶領域６２から抽出されるが、コンピュータ１０が図２に示すようなネットワーク化環境にあるならば、プリンタ公開鍵２５をサーバ３０の固定ディスク３１から抽出することができる。その後、復号化プリンタ公開鍵７５と、記憶領域６２から抽出したプリンタ公開鍵２５とを鍵検証アルゴリズム７７に提供してプリンタ公開鍵２５の信頼性を検証する。鍵検証アルゴリズム７７が、復号化プリンタ公開鍵７５はプリンタ公開鍵２５と一致すると判定した場合、プリンタ公開鍵２５は正規のものであり、場合に応じてプリンタ２０又はサーバ３０から最初に取得して以来、変更又は改変が行われていないことになる。もし不一致ならば、使用前にサーバ３０から取得した場合にプリンタ公開鍵２５が改変又は変更されたことになる。そのため、プリンタドライバ６０がコンピュータ１０のディスプレイ１１に表示するためにエラーメッセージを生成し、場合に応じてプリンタ２０又はサーバ３０からプリンタ公開鍵２５の新たな認証済みのコピーを再度取得するようにユーザを促すのが好ましい。

【００３９】図５Ｂは、プリンタ公開鍵２５の使用に先立ってプリンタ公開鍵２５の信頼性を検証するために図４Ｂに示すように作成して格納したデジタル署名７０の使用を示すブロック図である。図５Ｂにおいて、印刷コマンド７２はコンピュータ１０のユーザから受信するが、所望のプリントデータを機密にプリンタ２０に送るという指示を含んでいるのが好ましい。図５Ｂに示すように、ユーザ固有の公開鍵５３には、前述のようにオペレーティングシステム４０を介してアクセスするのが好ましい。ユーザ固有の公開鍵５３をデジタル署名７０と共に復号化アルゴリズム７６に提供して復号化プリンタ

公開鍵ハッシュ値７９を取得する。プリンタ公開鍵２５は記憶領域６２から抽出されるが、コンピュータ１０が図２に示すようなネットワーク化環境にあるならば、プリンタ公開鍵２５をサーバ３０の固定ディスク３１から抽出することができる。

【００４０】その後、プリンタ公開鍵２５に対してハッシングアルゴリズム６８を再度行い、新たなプリンタ公開鍵ハッシュ値８０を生成する。そして、復号化プリンタ公開鍵ハッシュ値７９と新たなプリンタ公開鍵ハッシュ値８０とをハッシュ検証アルゴリズム８４に提供してプリンタ公開鍵２５の信頼性を検証する。ハッシュ検証アルゴリズム８４が、復号化プリンタ公開鍵ハッシュ値７９は新たなプリンタ公開鍵ハッシュ値８０と一致すると判定した場合、プリンタ公開鍵２５は正規のものであり、場合に応じてプリンタ２０又はサーバ３０から最初に取得して以来、変更又は改変が行われていないことになる。もし不一致ならば、プリンタ公開鍵２５は改変又は変更されていることになる。例えば、最初にコンピュータ１０がサーバ３０からプリンタ公開鍵２５のバージョンを取得して以来、プリンタ公開鍵２５の新しいバージョンが作成されてプリンタ２０からサーバ３０にアップロードされている可能性もある。そのため、プリンタドライバ６０がコンピュータ１０のディスプレイ１１に表示するためにエラーメッセージを生成し、場合に応じてプリンタ２０又はサーバ３０からプリンタ公開鍵２５の新たな認証済みのコピーを再度取得するようにユーザを促すのが好ましい。

【００４１】図６は、プリンタ公開鍵２５が正規のものであると判定された場合のプリントデータの暗号化を説明するための図である。図６に示すように、ランダム鍵生成器８２を使用して対称鍵８３を生成する。対称鍵８３はデータオブジェクトを暗号化及び復号化するのに使用できる暗号化鍵である。ランダム鍵生成器８２はオペレーティングシステム４０の関数であるのが好ましく、関数呼出しによってアクセスされる。プリントデータ８５と対称鍵８３とを暗号化アルゴリズム６５に提供して暗号化プリントデータ８７を生成する。この点に関して、プリンタ２０は、印刷用に暗号化プリントデータ８７を復号化するために対称鍵８３の機密コピーが必要となる。このため、プリンタ公開鍵２５と対称鍵８３とを暗号化アルゴリズム６５に提供して暗号化対称鍵８８を生成する。このように、対称鍵を機密にプリンタ２０に渡すことができる。その後、暗号化対称鍵８８をプリントジョブ８９のヘッダ９０に配置するが、プリントジョブ８９は暗号化プリントデータ８７も含んでいる。プリントジョブ８９は接続１を介してプリンタ２０に送られる。プリントジョブ８９がプリンタ２０に向かう途中で傍受されても、プリンタ２０に機密に格納されたプリンタ秘密鍵２３を使用せずに暗号化対称鍵８８を復号化することはできないので、暗号化プリントデータ８７を適切に復号化することはできない。

【００４２】図７はプリンタ２０内の暗号化プリントデータ８７の復号化を説明するための図である。図７に示すように、プリントジョブ８９はプリンタ２０で受信される。プリンタ秘密鍵２３にはプリンタ２０の固定記憶装置２１からアクセスして、対称鍵８３を抽出するためにプリントジョブヘッダ９０からの暗号化対称鍵８８と共に復号化アルゴリズム９２に提供する。平文のプリントデータ８５を生成するために、対称鍵８３を暗号化プリントデータ８７と共に復号化アルゴリズム９２に提供する。その後、プリントデータ８５をプリンタ２０のプリントエンジン２７に渡して、プリンタ２０が記録媒体に印刷出力を生成して印刷画像１００を作成する。このように、プリンタ公開鍵２５の信頼性の検証に外部の認証局を使用することなく、プリンタ公開鍵２５を使用してプリントデータを毎回、機密にプリンタ２０に渡す。

【００４３】図８は、本実施の形態に係る公開鍵、特にプリンタ公開鍵の使用を説明するためのフローチャートである。ステップＳ８０１において、ユーザは、好ましくはパスワードを使用して、コンピュータ１０にログオンする。説明の便宜上、ユーザ１を例示するが、ユーザ１はログインＩＤ４５を提供してコンピュータ１０を使用する権限があることを検証する。次に、ステップＳ８０２において、ユーザ固有の鍵対５１をユーザ１の識別に基づいて鍵データベース５０から取得する。ステップＳ８０３において、プリンタ２０から（コンピュータ１０が図２に示すようなネットワーク化環境にあるならば、サーバ３０から）コンピュータ１０にプリンタ公開鍵２５を送る。プリンタ公開鍵２５は、場合に応じてプリンタ２０又はサーバ３０にコンピュータ１０から送られた鍵要求に応じて送出するのが好ましい。ステップＳ８０４において、場合に応じてプリンタ２０又はサーバ３０からプリンタ公開鍵２５を受信する。ステップＳ８０５において、図４Ｂを参照して説明したようにプリンタ公開鍵２５に署名するのが好ましいが、代わりに、図４Ａを参照して説明したようにプリンタ公開鍵２５を暗号化しても良い。

【００４４】ステップＳ８０５におけるこの２つの可能性を図９及び１０にそれぞれ示す。図９に示すように、ユーザ固有の秘密鍵５４を使用して暗号化アルゴリズム６５に沿ってプリンタ公開鍵２５を完全に暗号化することによって、暗号化プリンタ公開鍵６７を作成する（Ｓ９０１）。その後、フローは図９の「戻る」（Ｓ９０２）に進む。図１０に示すように、ハッシングアルゴリズム６８をプリンタ公開鍵２５に適用してプリンタ公開鍵ハッシュ値６９を作成する（Ｓ１００１）。ステップＳ１００２において、プリンタ公開鍵ハッシュ値６９をユーザ固有の秘密鍵５４で暗号化してデジタル署名７０を作成する。その後、フローは図１０の「戻る」（Ｓ１００３）に進む。

【００４５】図８に戻ると、フローはステップＳ８０６に進み、プリンタ公開鍵２５を今後も使用するために記憶領域６２に格納し、デジタル署名７０（または暗号化プリンタ公開鍵６７）をレジストリ４１に機密に格納する。代わりに、コンピュータ１０が図２に示すようにサーバ３０を有するネットワーク化環境にある場合は、プリンタ公開鍵２５を記憶領域６２に格納する代わりにサーバ３０の固定ディスク３１に格納できることは理解されるであろう。前述のように、コンピュータ１０が図２に示すようにネットワーク化計算環境にある場合は、プリンタ公開鍵２５をサーバ３０の固定ディスク３１に格納できる。このような場合、コンピュータ１０がこれ以降にデータを暗号化する必要がある度に、コンピュータ１０がサーバ３０からプリンタ公開鍵２５にアクセスするのが好ましい。これによって、サーバ３０に格納されたプリンタ公開鍵２５のバージョンがシステム管理者によって更新されたことをプリンタドライバが自動的に検出することが可能となる。ステップＳ８０７において、コンピュータ１０はユーザ１から印刷コマンド７２を受信するが、印刷コマンド７２はプリントデータを機密にプリンタ２０に送るという指示を含んでいるのが好ましい。

【００４６】次に、プリンタ公開鍵２５を、場合に応じて記憶領域６２又はサーバ３０の固定ディスク３１から抽出する（ステップＳ８０８）。ステップＳ８０９において、デジタル署名７０又は暗号化プリンタ公開鍵６７を復号化し、プリンタ公開鍵２５と共に検証アルゴリズムに提供してプリンタ公開鍵２５の信頼性を検証する。図９及び１０を参照して説明したように、プリンタ公開鍵２５に署名するのか又は完全に暗号化するのかによってこのステップは異なる。図１１はプリンタ公開鍵２５を完全に暗号化する場合のステップＳ８０９の説明を示す。ステップＳ１１０１において、ユーザ固有の公開鍵５３を使用して、レジストリ４１から抽出した暗号化プリンタ公開鍵６７を復号化する。次に、ステップＳ１１０２において、復号化プリンタ公開鍵７５と抽出したプリンタ公開鍵２５とを、それらが一致しているかどうかを検証するための鍵検証アルゴリズム７７に提供することによって、プリンタ公開鍵２５は正規のものであり、プリントデータを適切に暗号化するのに使用できると判定する。その後、フローはステップＳ１１０３の「戻る」に進む。

【００４７】図１２はプリンタ公開鍵２５にデジタル署名してデジタル署名７０を作成する場合を示す。ステップＳ１２０１において、ユーザ固有の公開鍵５３を使用して、レジストリ４１から抽出したデジタル署名７０を復号化することによって、復号化プリンタ公開鍵ハッシュ値７９を取得する。次に、ステップＳ１２０２において、新たなプリンタ公開鍵ハッシュ値８０を取得するために、場合に応じて記憶領域６２又はサーバ３０から抽出したプリンタ公開鍵２５にハッシングアルゴリズム６８を適用する。ステップＳ１２０３において、復号化プリンタ公開鍵ハッシュ値７９と新たなプリンタ公開鍵ハッシュ値８０とをハッシュ検証アルゴリズム８４に提供してこれら２つのハッシュ値が一致するかどうかを判定し、これによってプリンタ公開鍵２５の信頼性を確認する。その後、フローはステップＳ１２０４の「戻る」に進む。

【００４８】図８に戻ると、フローはステップＳ８１０に進み、ステップＳ８０９で行われた検証で一致していたかを判定する。一致していたならば、フローはステップＳ８１２に進む。一致していないならば、フローはステップＳ８１１に進み、コンピュータ１０のディスプレイ１１に表示するためにエラーメッセージを生成した後、ステップＳ８１９の「戻る」に進む。ステップＳ８１２において、ランダム鍵生成器８２を使用して対称鍵８３を生成する。ステップＳ８１３において、暗号化アルゴリズム６５を使用して対称鍵８３でプリントデータ８５を暗号化して暗号化プリントデータ８７を生成する。次に、ステップＳ８１４において、暗号化アルゴリズム６５を使用して検証済みのプリンタ公開鍵２５で対称鍵８３を暗号化して暗号化対称鍵８８を生成する。暗号化対称鍵８８と暗号化プリントデータ８７とをプリントジョブ８９に配置してプリンタ２０に送る（ステップＳ８１５）。その後、フローはステップＳ８１６に進み、プリンタ２０はプリントジョブ８９を受信し、復号化アルゴリズム９２を介してプリンタ秘密鍵２３を適用して暗号化対称鍵８８を復号化し、これによって対称鍵８３を抽出する。対称鍵８３を暗号化プリントデータ８７に適用して復号化（明文の）プリントデータ８５を抽出する（ステップＳ８１７）。復号化プリントデータ８５はプリンタ２０のプリントエンジン２７に送られて、プリントデータ８５に基づき印刷画像１００を生成する（ステップＳ８１８）。その後、フローはステップＳ８１９の「戻る」に進む。

【００４９】図１３は、プリンタ２０から受信したプリンタ公開鍵２５などの受信公開鍵の初期認証のための本実施の形態に係る好適な構成を示す。特に、コンピュータ１０がプリンタ公開鍵２５の正しいコピーを受信したことを確認するために、プリンタ公開鍵２５をコンピュータ１０が最初に取得する場合に本構成によって認証を行う。図１３に示すように、プリンタ公開鍵２５をプリンタ２０から取得してハッシングアルゴリズム６８を行い、プリンタ公開鍵ハッシュ値６９を生成する。

【００５０】次に、好ましくは、コンピュータ１０のユーザによってプリンタ２０の前面で入力されたコマンドに応じて、プリンタテストページ１０２をプリンタ２０で生成する。プリンタテストページは、プリンタ公開鍵２５に対する正しいハッシュ値である印刷ハッシュ値１０３を含んでいる。印刷ハッシュ値１０３はユーザによ

ってコンピュータ１０に入力されて、プリンタ公開鍵ハッシュ値６９と共にハッシュ検証アルゴリズム８４に提供される。このハッシュ検証アルゴリズム８４は、受信したプリンタ公開鍵２５の信頼性を検証するためにこれら２つのハッシュ値が一致するかどうかを判定する。一致するならば、コンピュータ１０はプリンタ公開鍵２５をプリンタ２０からの正規のコピーとして受け付け、今後も使用するためにプリンタ公開鍵２５を記憶領域６２に格納する。一致しないならば、コンピュータ１０のディスプレイ１１に表示するためにエラーメッセージを生成し、プリンタ公開鍵２５に対して他の要求をプリンタ２０に送る又は印刷ハッシュ値１０３をコンピュータ１０に再入力するなどの行動を起こすようにユーザを促す。

【００５１】図１４は、図１３に示すプリンタ公開鍵２５の初期認証を説明するためのフローチャートである。ステップＳ１４０１において、プリンタ公開鍵２５をプリンタ２０から要求する。ステップＳ１４０２において、プリンタ２０はプリンタ公開鍵２５をコンピュータ１０に送る。プリンタ公開鍵２５に対してハッシングアルゴリズム６８を行い、プリンタ公開鍵ハッシュ値６９を生成する（ステップＳ１４０３）。次に、好ましくは、コンピュータ１０のユーザによってプリンタ２０の前面で入力されたコマンドに応じて、プリンタテストページ１０２をプリンタ２０で生成する。このプリンタテストページは、プリンタ公開鍵２５に対する正しいハッシュ値である印刷ハッシュ値１０３を含んでいる。

【００５２】ステップＳ１４０５において、好ましくは、コンピュータ１０のディスプレイ１１上に提供されたダイアログウィンドウから、印刷ハッシュ値１０３がユーザによってコンピュータ１０に入力される。ステップＳ１４０６において、印刷ハッシュ値１０３はプリンタ公開鍵ハッシュ値６９と共にハッシュ検証アルゴリズム８４に提供される。ハッシュ検証アルゴリズム８４は、受信したプリンタ公開鍵２５の信頼性を検証するために、これら２つのハッシュ値が一致するかどうかを判定する。一致するならば、フローはステップＳ１４０９に進み、コンピュータ１０はプリンタ公開鍵２５をプリンタ２０からの正規のコピーとして受け付け、今後も使用するためにプリンタ公開鍵２５を記憶領域６２に格納する。その後、フローはステップＳ１４１０に進む。ステップＳ１４０７において一致しないならば、フローはステップＳ１４０８に進み、コンピュータ１０のディスプレイ１１に表示するためにエラーメッセージを生成し、プリンタ公開鍵２５に対して他の要求をプリンタ２０に送る又は印刷ハッシュ値１０３をコンピュータ１０に再入力するなどの行動を起こすようにユーザを促す。その後、フローはステップＳ１４１０の「戻る」に進む。

【００５３】このように、暗号化するために公開鍵が必要になる度に外部の認証局を使用して公開鍵の信頼性を検証する必要がなく、公開鍵の使用を通じて機密印刷を提供する。特に、プリンタの公開鍵などの対象公開鍵を今後も使用するためにコンピュータに機密に保持してデータを暗号化することができる。そのため、対象公開鍵の暗号化（署名）とそれ以降の検証を、局所的に保持されたユーザ固有の公開鍵で局所的に行うことによって、使用する前に毎回、対象公開鍵の信頼性を検証することが容易になる。

【００５４】以上説明したように本実施形態の一つの側面によれば、暗号化するために公開鍵が必要になる度に外部の認証局に問い合わせて公開鍵の信頼性を検証する必要がなくなる。

【００５５】また、本願実施形態の別の側面によれば、負荷の小さな処理で機密性の高い通信処理又はデータ処理環境を提供することができる。

【００５６】

【発明の効果】以上説明したように本発明によれば、暗号化するために公開鍵が必要になる度に外部の認証局に問い合わせて公開鍵の信頼性を検証する必要がなくなるという効果がある。

【００５７】本発明を特定の実施例によって説明した。本発明は上述の実施の形態には限定されず、当業者により本発明の趣旨から逸脱せずに様々な変更及び変形を実施しうることは理解されるであろう。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る計算環境を表す図である。

【図２】本発明の他の実施の形態に係るネットワーク化計算環境を表す図である。

【図３】図１に示すコンピュータ及びプリンタの内部構造を示す詳細なブロック図である。

【図４Ａ】本発明の一実施の形態に係る公開鍵の暗号化を説明するためのブロック図である。

【図４Ｂ】本発明の他の実施の形態に係る公開鍵の暗号化を説明するためのブロック図である。

【図５Ａ】本発明の一実施の形態に係る格納済みの公開鍵の検証を説明するためのブロック図である。

【図５Ｂ】本発明の他の実施の形態に係る格納済みの公開鍵の検証を説明するためのブロック図である。

【図６】本実施の形態に係るプリントデータの暗号化を説明するためのブロック図である。

【図７】本実施の形態に係るプリントデータの復号化を説明するためのブロック図である。

【図８Ａ】本発明の実施の形態に係る公開鍵の使用を説明するためのフローチャートである。

【図８Ｂ】本発明の実施の形態に係る公開鍵の使用を説明するためのフローチャートである。

【図９】本発明の一実施の形態に係る公開鍵の暗号化を説明するためのフローチャートである。

【図１０】本発明の他の実施の形態に係る公開鍵の署名を説明するためのフローチャートである。
【図１１】本発明の一実施の形態に係る格納済みの公開鍵の検証を説明するためのフローチャートである。
【図１２】本発明の他の実施の形態に係る格納済みの公開鍵の検証を説明するためのフローチャートである。
【図１３】本発明の一実施の形態に係る受信公開鍵の初期検証を説明するためのブロック図である。
【図１４】本発明の一実施の形態に係る受信公開鍵の初期検証を説明するためのフローチャートである。

【図1】

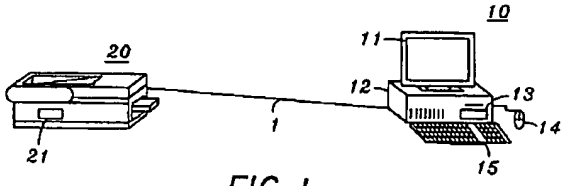

FIG. 1

【図2】

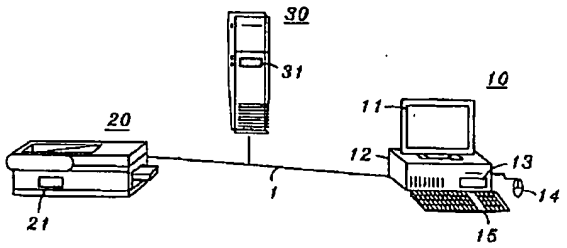

FIG. 2

【図3】

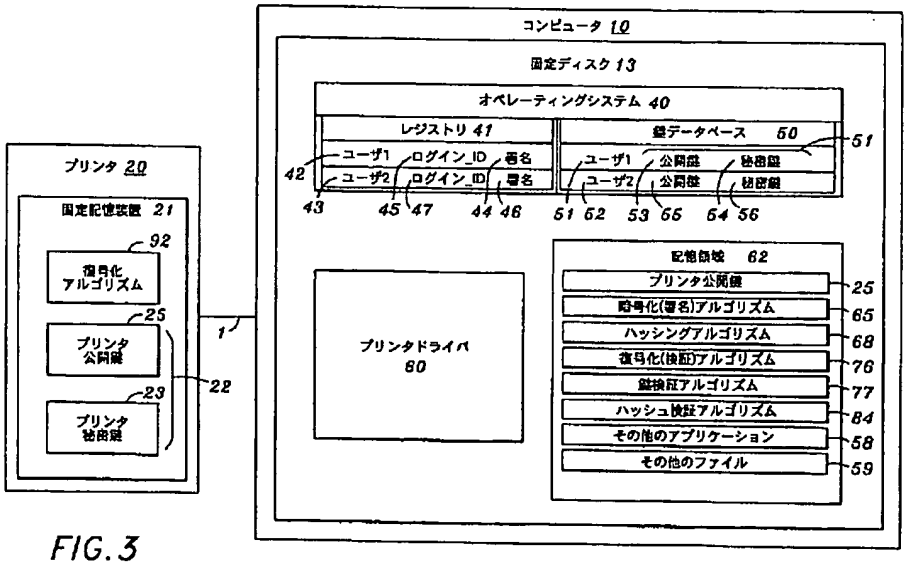

FIG. 3

【図４Ａ】

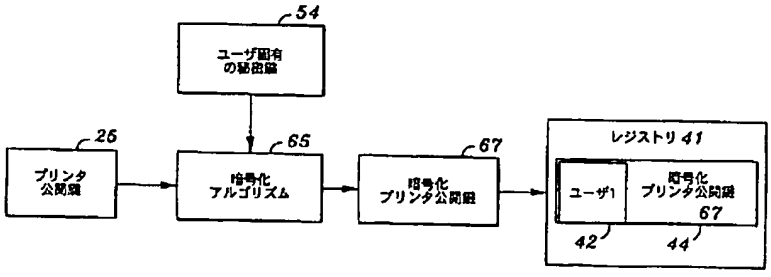

FIG. 4A

【図４Ｂ】

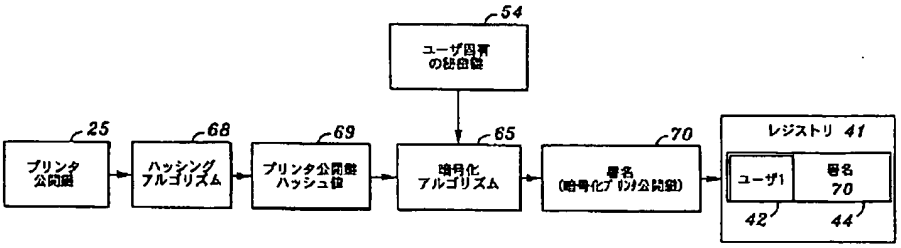

FIG.4B

【図５Ａ】

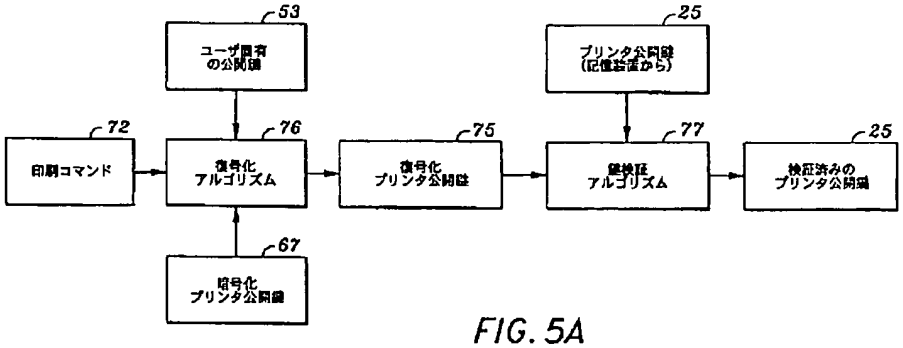

FIG. 5A

【図５Ｂ】

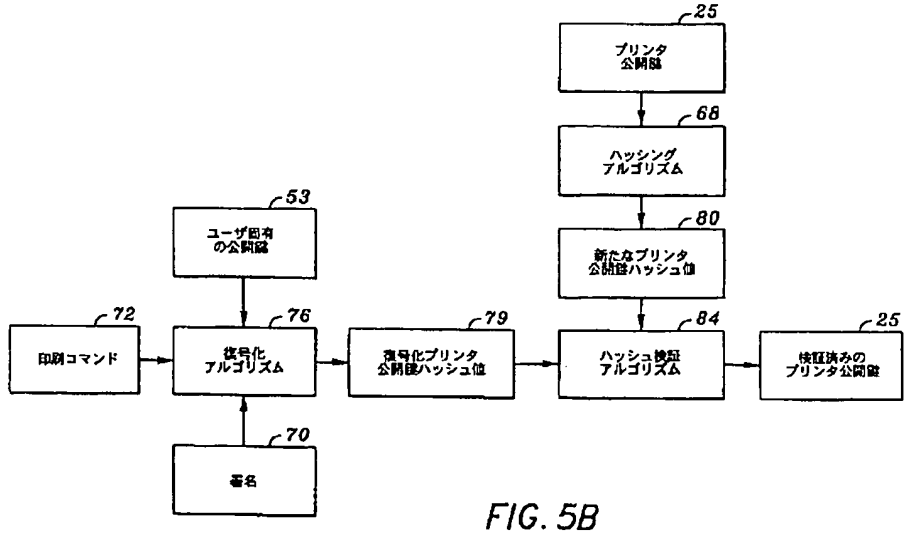

FIG. 5B

【図6】

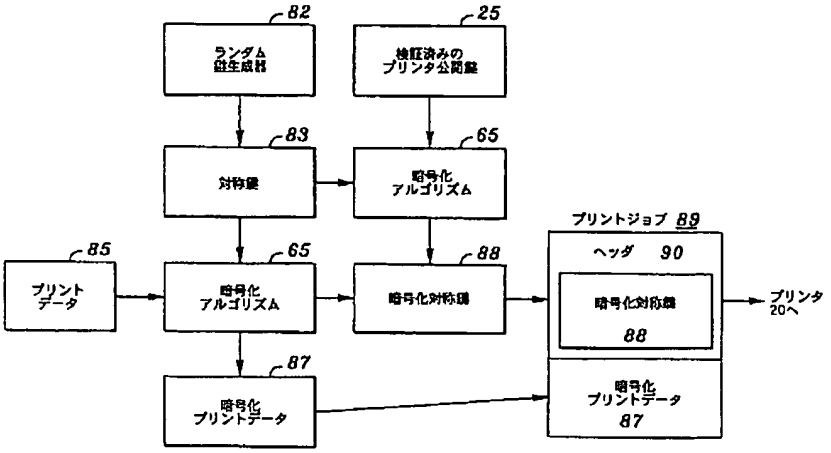

FIG. 6

【図7】

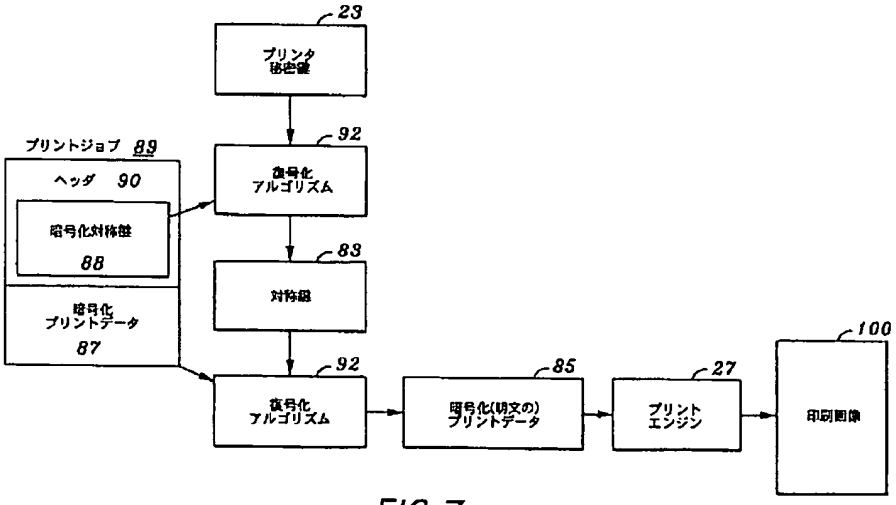

FIG. 7

【図8A】

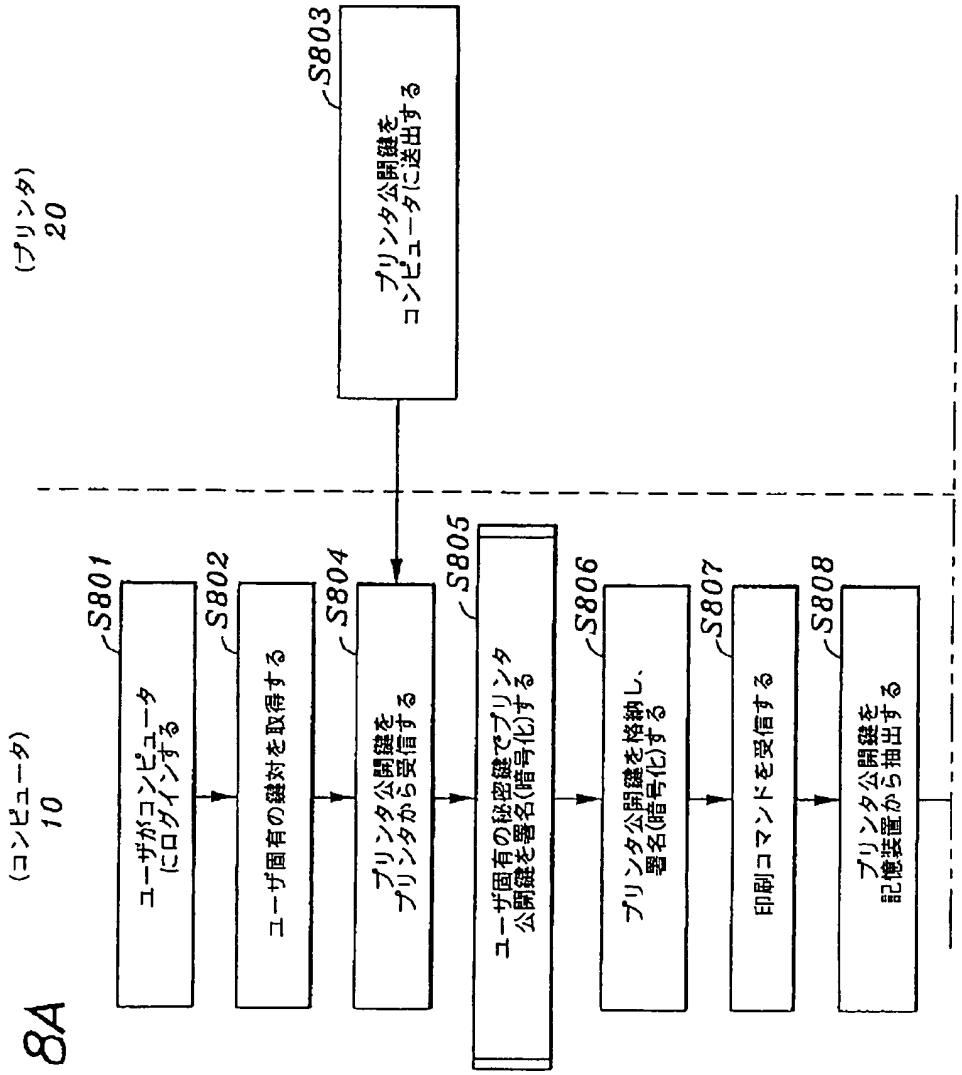
(プリンタ)
20
(コンピュータ)
10
S801
ユーザがコンピュータにログインする
S802
ユーザ固有の鍵対を取得する
S803
プリンタ公開鍵をコンピュータに送出する
S804
プリンタ公開鍵をプリンタから受信する
S805
ユーザ固有の秘密鍵でプリンタ公開鍵を署名(暗号化)する
S806
プリンタ公開鍵を署名(暗号化)する
S807
印刷コマンドを受信する
S808
プリンタ公開鍵を記憶装置から抽出する

FIG. 8A

【図8B】

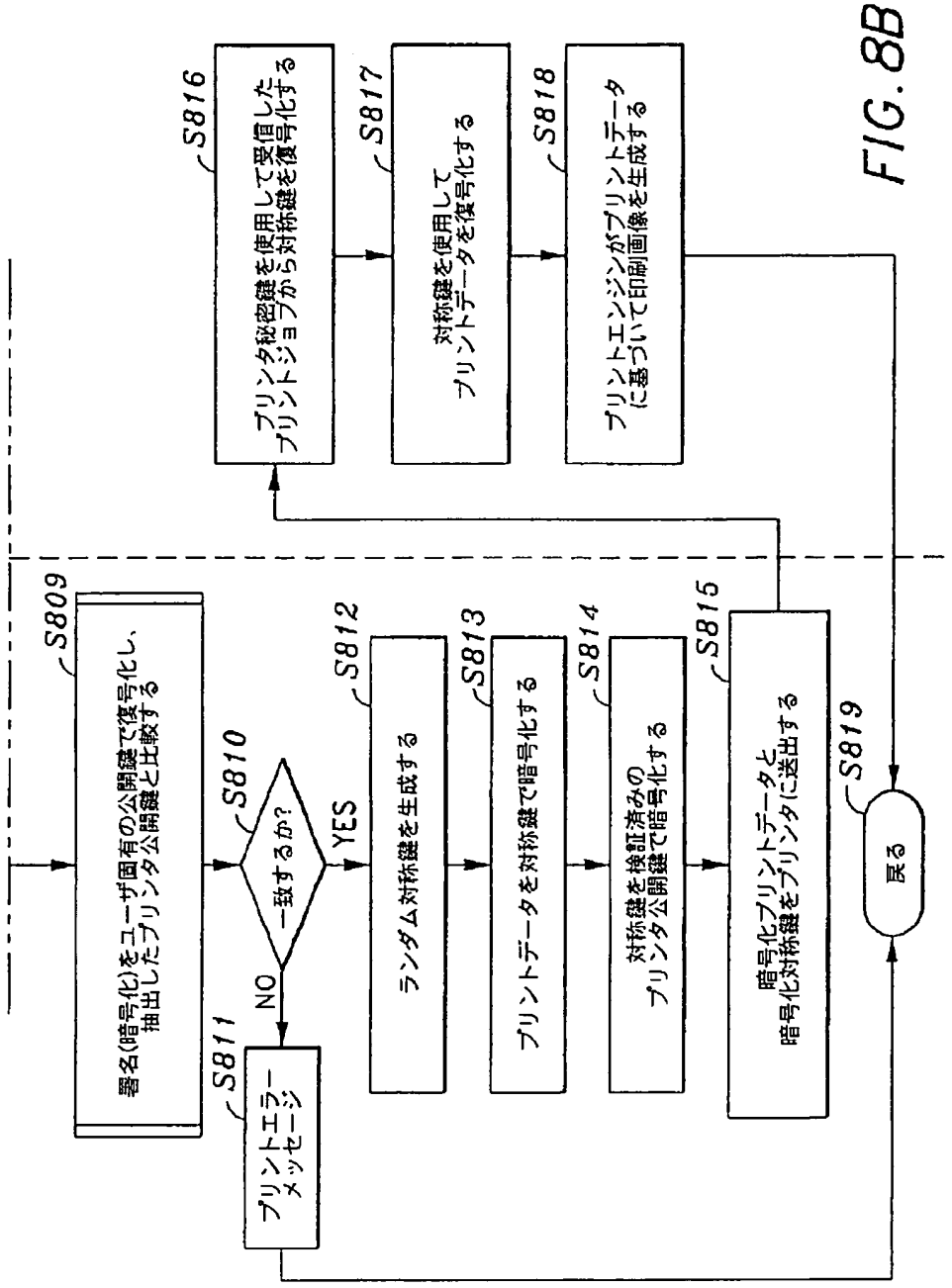
S809
暑名(暗号化)をユーザ固有の公開鍵で復号化し、
抽出したプリンタ公開鍵と比較する
S810
一致するか?
YES
NO
S811
プリントエラー
メッセージ
S812
ランダム対称鍵を生成する
S813
プリントデータを対称鍵で暗号化する
S814
対称鍵を検証済みの
プリンタ公開鍵で暗号化する
S815
暗号化プリントデータと
暗号化対称鍵をプリンタに送出する
S816
プリンタ秘密鍵を使用して受信した
プリントジョブから対称鍵を復号化する
S817
対称鍵を使用して
プリントデータを復号化する
S818
プリントエンジンがプリントデータ
に基づいて印刷画像を生成する
S819
戻る

FIG. 8B

【図9】

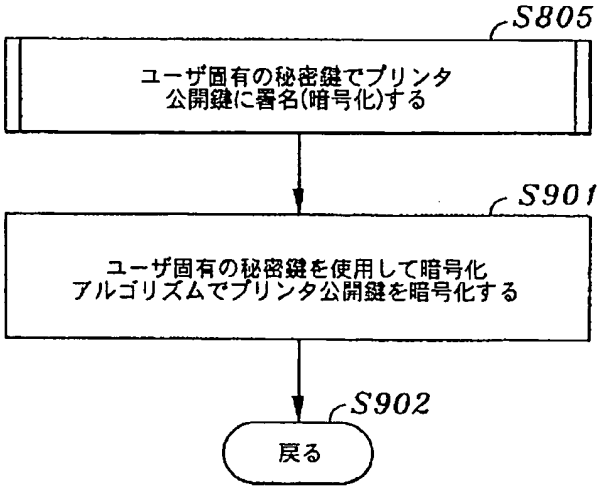

FIG. 9

【図10】

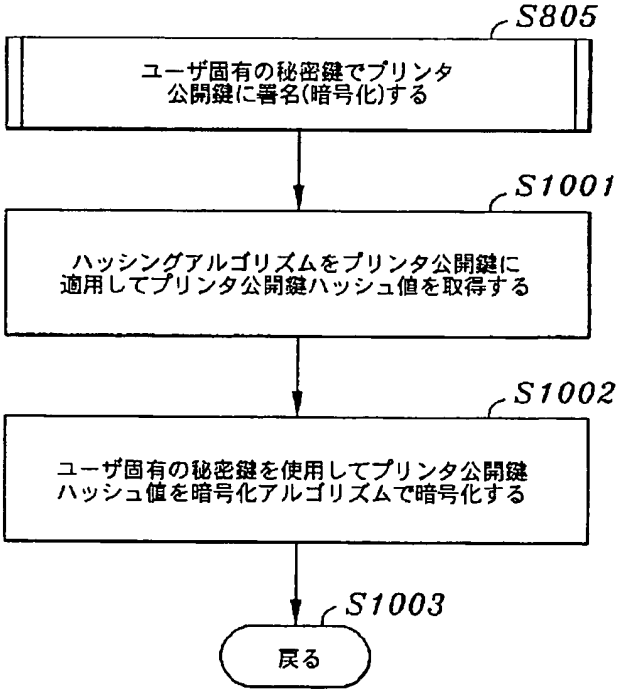

FIG. 10

【図11】

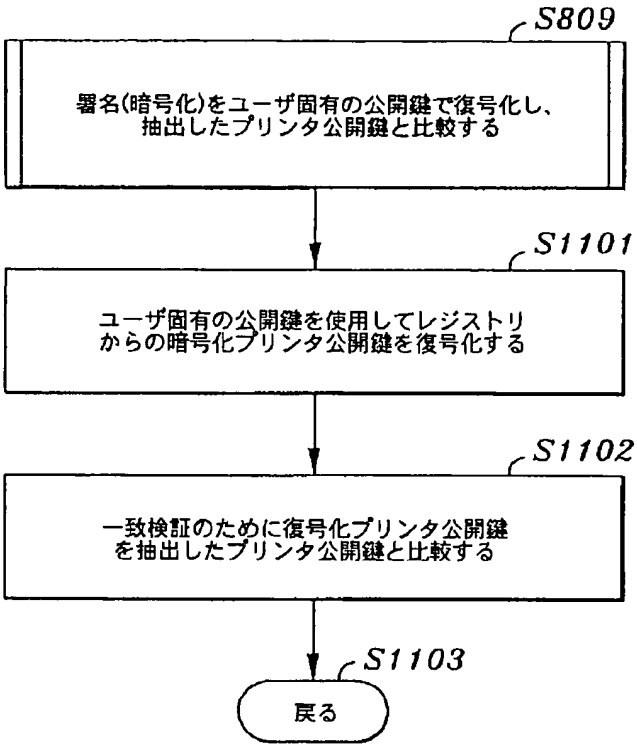

FIG. 11

【図13】

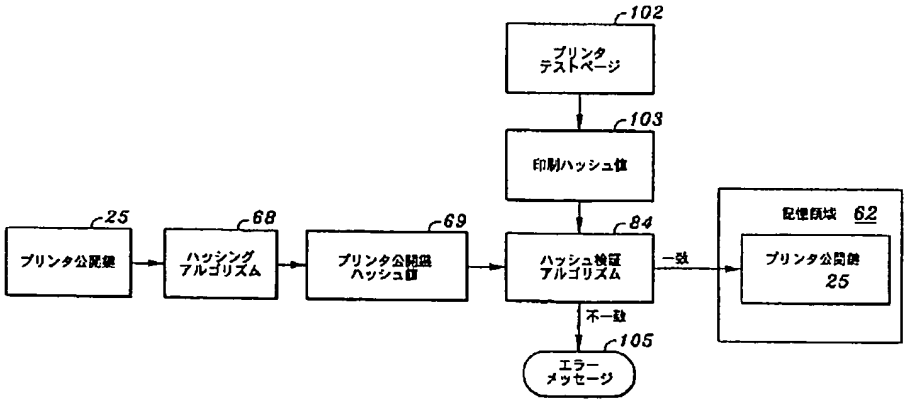

FIG. 13

【図12】

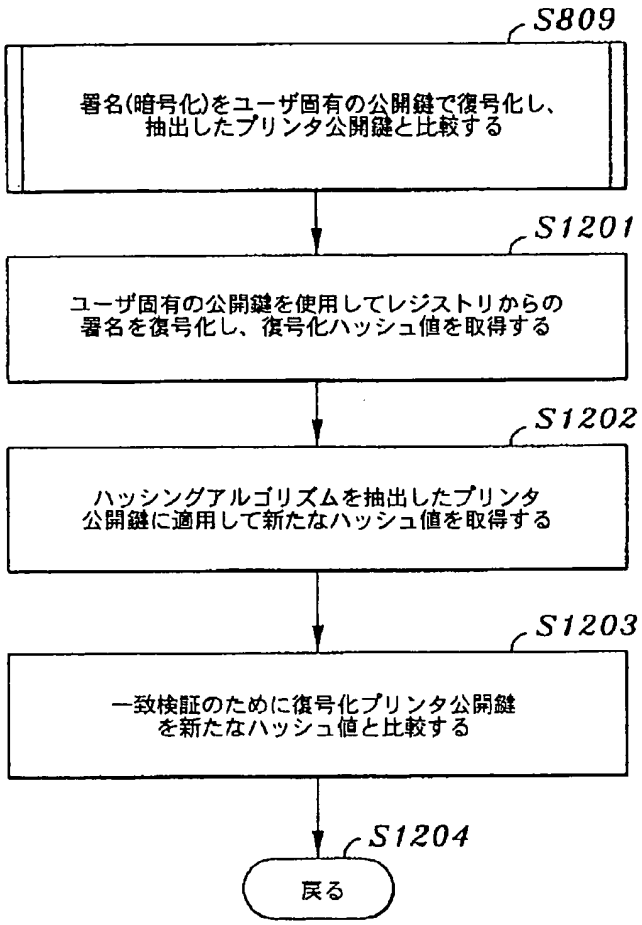
S809
署名(暗号化)をユーザ固有の公開鍵で復号化し、
抽出したプリンタ公開鍵と比較する
S1201
ユーザ固有の公開鍵を使用してレジストリからの
署名を復号化し、復号化ハッシュ値を取得する
S1202
ハッシングアルゴリズムを抽出したプリンタ
公開鍵に適用して新たなハッシュ値を取得する
S1203
一致検証のために復号化プリンタ公開鍵
を新たなハッシュ値と比較する
S1204
戻る

FIG. 12

【図14】

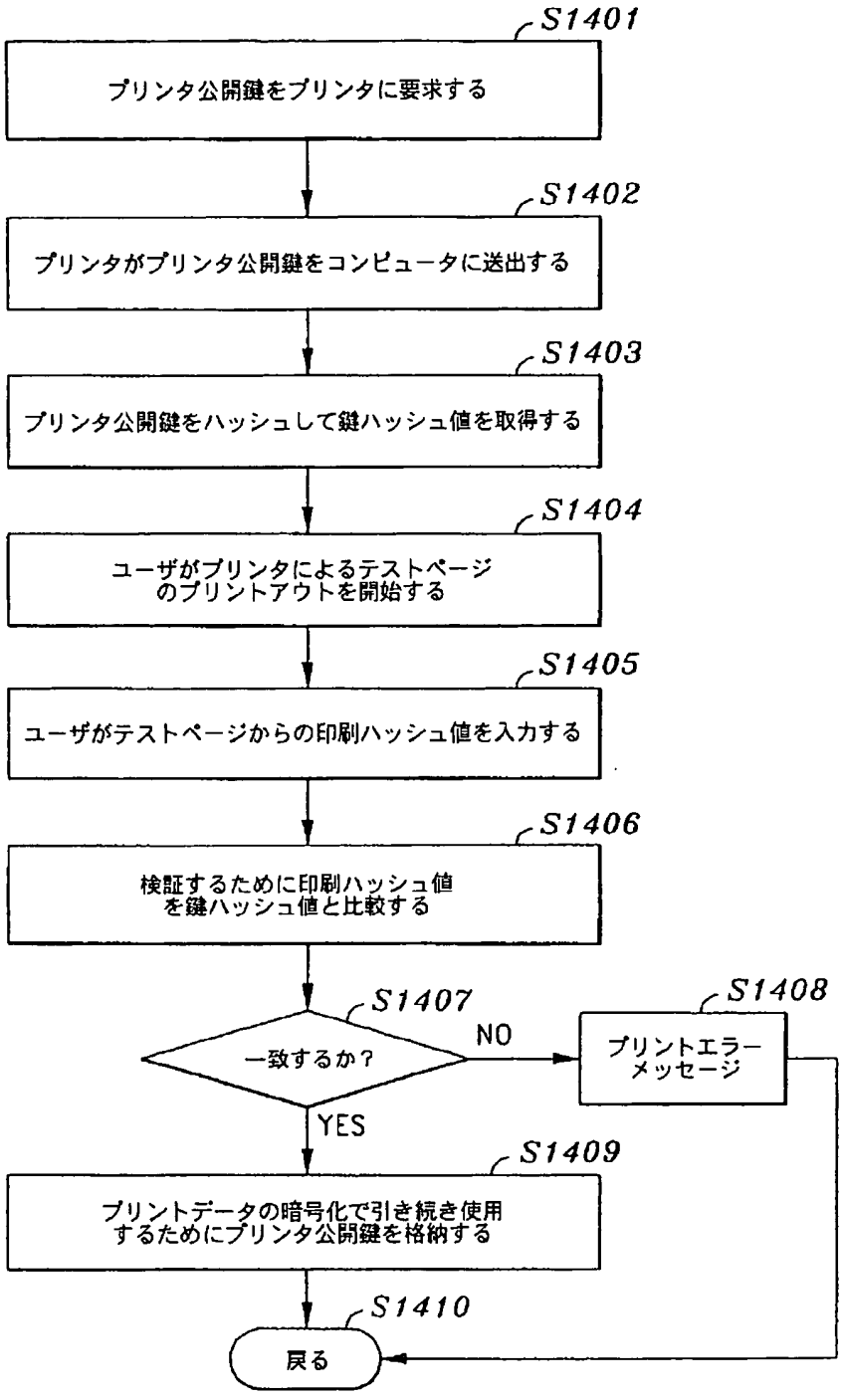
S1401
プリンタ公開鍵をプリンタに要求する
S1402
プリンタがプリンタ公開鍵をコンピュータに送出する
S1403
プリンタ公開鍵をハッシュして鍵ハッシュ値を取得する
S1404
ユーザがプリンタによるテストページのプリントアウトを開始する
S1405
ユーザがテストページからの印刷ハッシュ値を入力する
S1406
検証するために印刷ハッシュ値を鍵ハッシュ値と比較する
S1407
一致するか?
NO
S1408
プリントエラーメッセージ
YES
S1409
プリントデータの暗号化で引き続き使用するためにプリンタ公開鍵を格納する
S1410
戻る

FIG. 14

フロントページの続き

(72)発明者 ウイリアム ツァン
アメリカ合衆国 カリフォルニア州 92612, アーバイン, イノベーション ドライブ 110 キヤノン デベロップメント アメリカス, インコーポレイテッド内
(72)発明者 ドン フランシス パープラ
アメリカ合衆国 カリフォルニア州 92612, アーバイン, イノベーション ドライブ 110 キヤノン デベロップメント アメリカス, インコーポレイテッド内
(72)発明者 ニール ワイ. イワモト
アメリカ合衆国 カリフォルニア州 92612, アーバイン, イノベーション ドライブ 110 キヤノン デベロップメント アメリカス, インコーポレイテッド内
(72)発明者 クレイグ マザガット
アメリカ合衆国 カリフォルニア州 92612, アーバイン, イノベーション ドライブ 110 キヤノン デベロップメント アメリカス, インコーポレイテッド内

Fターム(参考) 5B017 AA03 BB09 CA16
5B021 AA30 BB09 CC05
5J104 AA09 AA16 EA05 LA03 LA06